



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

2131  
#4

In re application of: **Black et al.**

Serial No.: **09/942,633**

Filed: **August 20, 2001**

For: **Hierarchical Correlation of  
Intrusion Detection Events**

§ Group Art Unit: **2131**  
§  
§ Examiner: **Unknown**  
§  
§ Attorney Docket No.: **AUS920010244US1**  
§

**Certificate of Mailing Under 37 C.F.R. § 1.8(a)**  
I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to:  
Assistant Commissioner of Patents, Washington, D.C. 20231 on \_\_\_\_  
01-07-02  
By: Dell Whitton  
Dell Whitton

**RECEIVED**

**TRANSMITTAL DOCUMENT**

**FEB 04 2002**

Assistant Commissioner of Patents  
Washington, D.C. 20231

**Technology Center 2100**

Sir:  
ENCLOSED HEREWITH:

- Information Disclosure Statement;
- Form PTO-1449;
- References AA-AF; and
- Our return postcard.

No fees are believed to be necessary. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee

Duke W. Yee

Registration No. 34,285

**CARSTENS, YEE & CAHOON, LLP**

P.O. Box 802334

Dallas, Texas 75380

(972) 367-2001

**ATTORNEY FOR APPLICANT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**RECEIVED**

In re application of: **Black et al.** §  
 Serial No.: **09/942,633** §  
 Filed: **August 30, 2001** §  
 For: **Hierarchical Correlation of** §  
**Intrusion Detection Events** §



Group Art Unit: **2131**

FEB 04 2002

Examiner: **Unknown**

Technology Center **2100**

Attorney Docket No.: **AUS920010244US1**

**INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. 1.97**

Hon. Assistant Commissioner of Patents  
 Washington, D.C. 20231

Sir:

Applicants request that the information listed on the attached Form PTO-1449 be considered by the Office during the pendency of the above entitled application, pursuant to 37 C.F.R. 1.97.

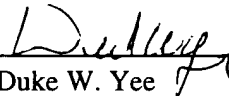
Please charge any fees necessary for prosecution of the present application to Deposit Account No. 09-0447. If any extension of time is required, such extension is hereby requested. Please charge any additional required fee for extension of time to Deposit Account No. 09-0447.

In accordance with 37 C.F.R. 1.97(h), the filing of this Information Disclosure Statement shall not constitute an admission that any information cited therein is, or is considered to be, material to patentability as defined in 37 C.F.R. 1.56(b). In the interest of full and complete disclosure to the Office, some or all of the art cited herein may not be considered by Applicant(s) or the Undersigned to be material under the new standards of materiality defined in 37 C.F.R. 1.56(b), enacted March 16, 1992, but may be material under the old standard of materiality defined in 37 C.F.R. 1.56(a), last amended on November 28, 1988, or may merely be technical background which may be of interest to the Examiner. In accordance with 37 C.F.R. 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made.

This Information Disclosure Statement is being filed under 37 C.F.R. § 1.97(b) within three months of the filing date of the application, or before the mailing date of a first office action on the merits. No fee is required.

Respectfully submitted,

Date: 1/7/02

  
Duke W. Yee  
Registration No. 34,285  
CARSTENS, YEE & CAHOON, LLP  
P.O. Box 802334  
Dallas, Texas 75380  
(972) 367-2001

**RECEIVED**

FEB 04 2002

#4

U.S. DEPT. OF COMMERCE PATENT AND TRADEMARK OFFICE

Technology Center 2100

Page 1 of 1

<b>Form PTO-1449</b>  <b>LIST OF PRIOR ART CITED BY APPLICANT</b> <i>(Use several sheets if necessary)</i>	ATTORNEY DOCKET NO. <b>AUS920010244US1</b>	SERIAL NO. <b>09/942,633</b>
	APPLICANT <b>Black et al.</b>	
	FILING DATE <b>August 30, 2001</b>	GROUP ART UNIT <b>2131</b>

**U.S. PATENT DOCUMENTS**

EXAMINER INITIAL	DOCUMENT NO.	PUBLICATION DATE	INVENTOR NAME	CLASS/ SUBCLASS	FILING DATE
	AA 5991881	Nov. 23, 1999	Conklin et al.	713/201	Nov. 8, 1996
	AB 5621889	Apr. 15, 1997	Lernuzeaux et al.	395/186	Jun. 8, 1994
	AC 5568471	Oct. 22, 1996	Hershey et al.	370/17	Sep. 6, 1995
	AD 5448722	Sep. 5, 1995	Lynne et al.	395/650	Mar. 10, 1993
	AE 5471194	Nov. 28, 1995	Guscott	340/511	Mar. 23, 1993

**FOREIGN PATENT DOCUMENTS**

EXAMINER INITIAL	DOCUMENT NO.		PUBLICATION DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES NO	
	AF	EP0985995A1	Mar. 15, 2000	Europe	G06F 1/00		X
	AG	WO 94/0739	Mar. 31, 1994	PCT	H04Q 9/00		X
	AH	JP11212831A	Aug. 6, 1999	Japan	G06F 11/34		X

**OTHER PRIOR ART (including author, title, date, pertinent page, etc.)**

AI	IBM Technical Disclosure Bulletin, "Dynamic Intrusion Detection for Secure Access Enclosure", Vol. 36, No. 06B, June 1993, pp. 233-235.
AJ	Hass, KJ et al., "On a Microcomputer Implementation of an Intrusion-Detection Algorithm", IEEE Transactions on Acoustics, Speech and Signal Processing, vol. ASSP-27, no. 6, pt. 2, pp. 782-789, Dec. 1979, abstract.
AK	Ming Yuh Huang et al., "A Large Scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis", Computer Networks, Vol. 31, No. 23-24, pp. 2465-2475, 14 Dec. 1999, Abstract.
AL	Kato, N et al., "A Real-Time Intrusion Detection System (IDS) for Large-Scale Networks and its Evaluations", IEICE Transactions on Communications, Vol. E82-B, No. 11, pp. 1817-1825, Nov. 1999, Abstract.
AM	Sekar, R et al., "On Preventing Intrusions by Process Behaviour Monitoring", Proceedings of the Workshop on Intrusion Detection and Network Monitoring (ID'99), pp. 29-40, Published: Berkeley, CA, USA, 1999, 140 pp., Abstract.
AN	Girardin, L., "An Eye on Network Intruder-Administrator Shootouts", Proceedings of the Workshop on Intrusion Detection and Network Monitoring (ID'99), pp. 19-28, Published: Berkeley, CA, USA, 1999, 140 pp., Abstract.
AO	Vigna, G et al., "NetSTAT: A Network-Based Intrusion Detection System", Journal of Computer Security, Vol. 7, No. 1, pp. 37-71, 1999, Abstract.
AP	Vigna, G et al., "NetSTAT: A Network-Based Intrusion Detection Approach", Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217), pp. 25-34, Published: Los Alamitos, CA, USA, 1998, xiii+365 pp., Abstract.
AQ	White, GB et al., "A Peer-Based Hardware Protocol for Intrusion Detection Systems", MILCOM 96. Conference Proceedings (Cat. No. 96CH36008), Pt. Vol. 2, pp. 468-472 vol. 2, Published: New York, NY, USA, 1996, 3 vol. xxiv+1083 pp., Abstract.
AR	Winkler, JR et al., "Intrusion and Anomaly Detection in Trusted Systems", Fifth Annual Computer Security Applications Conference (Cat. No. 89TH0287-3), pp. 39-45, Published: Los Alamitos, CA, USA, 1990, xv+357 pp., Abstract.

DATE CONSIDERED

EXAMINER

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP § 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.